

Exhibit 70

Excerpts of SW-SEC00264310

From: Johnson, Rani [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0EE57945F15E47B3ABAA99A59170AD3F-JOHNSON, RA]
Sent: 8/16/2019 5:42:59 PM
To: Joseph Kim (joe.kim@solarwinds.com) [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a3cc8cb2d6794a14ac4a9ed62a469cb7-kim, joe]; Kalsu, Bart [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=fc2ab67567ef49f384835b8ad9d94712-Kalsu, Bart]; Jason Bliss (Jason.Bliss@solarwinds.com) [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f3695c6e255040fb884d2752cd088540-Bliss, Jaso]; Pierce, Kellie [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0150ef14c7a24cb1a0e08ec9fcb06424-Pierce, Kel]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]; Zador, Jennifer [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=24b5eea9cfaa4c60b50f70ec7ed8b942-Zador, Jenn]
Subject: RE: Security & Compliance Q3 2019 Quarterly Review [Presentation]
Attachments: 082019Security_Compliance_Quarterly.pptx

Sensitivity: Company Confidential

Thanks for your time today. The presentation we reviewed is attached.
 Please advise if you have any questions / or would like additional information.



Rani Johnson | Chief Information Officer | **SolarWinds**

Office: 512.682.9541 | Mobile: 512.299.0610 | Wearable: 512.736.3400

-----Original Appointment-----

From: Hurley, Shirley **On Behalf Of** Johnson, Rani

Sent: Monday, April 29, 2019 3:32 PM

To: Johnson, Rani; Joseph Kim (joe.kim@solarwinds.com); Kalsu, Bart; Jason Bliss (Jason.Bliss@solarwinds.com); Pierce, Kellie; Murgia, Martha; Hurley, Shirley; Brown, Timothy; Zador, Jennifer

Subject: Security & Compliance QBR

When: Friday, August 16, 2019 9:30 AM-10:00 AM (UTC-06:00) Central Time (US & Canada).

Where: Exec conf room



SECURITY & COMPLIANCE PROGRAM QUARTERLY OVERVIEW

AUGUST 16, 2019



SolarWinds Scorecard

NIST Maturity Level



Security Category	2017	2018	2019
Identify	0.8	2.0	3.2
Protect	1.5	3.0	3.2
Detect	1.0	2.8	2.8
Respond	0.8	2.8	2.8
Recover	0.7	2.0	2.0
Overall	1.0	2.5	2.8

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds

9



IDENTIFY



Highlights

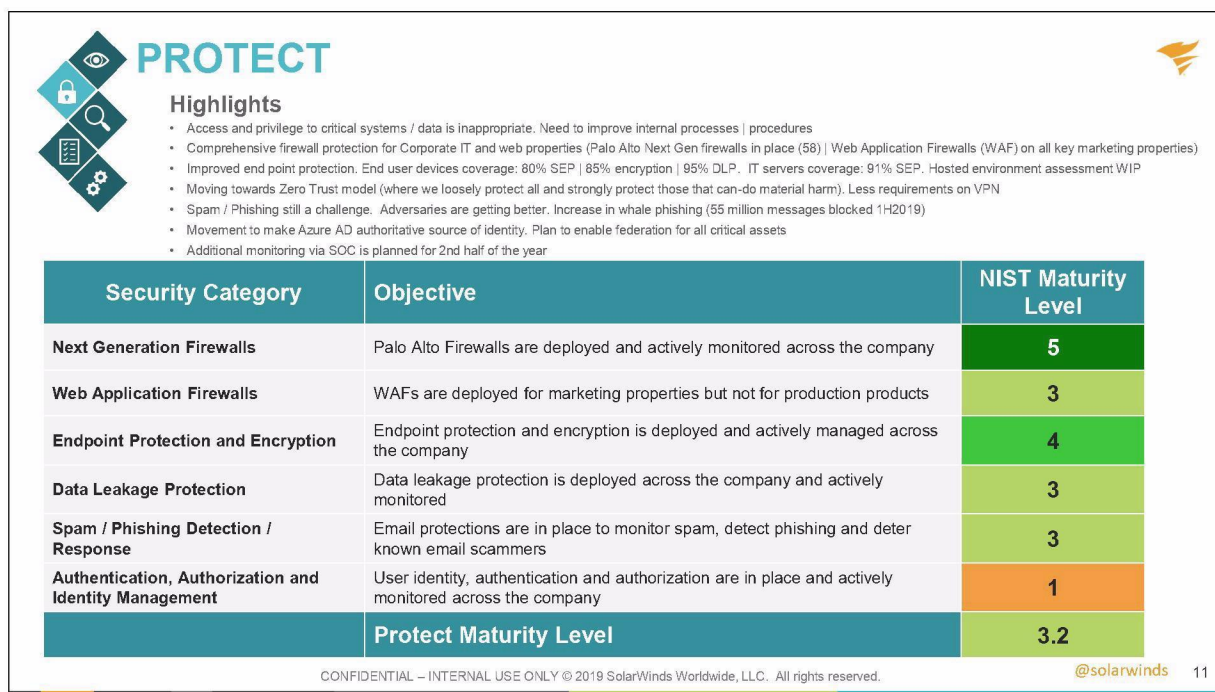
- Instituted standardized security scoring method (CVSS). 421 internally discovered issues marked security | 292 resolved in 1H 2019
- Open Source License Scanning coverage across entire portfolio
- Full lifecycle software asset management
- ISO certifications achieved for RMM, Backup, Take Control. N-central, Mail Assure (In progress), SOC 2 Type 1 for Passport, Loggly & App Optics (in progress)
- Threat intel ingestion remains a manual process

Security Category	Objective	NIST Maturity Level
Asset Management	Internally and externally facing assets are identified and actively managed	3
Secure Software Development Lifecycle (SSDL)	Employees are aware of and utilize a security software development lifecycle in their day to day activities	2
Open Source License Scanning	Open source code used is scanned and remediated as needed	3
Product Certifications	ISO 27001 information security management system (ISMS) framework of policies and procedures are followed and audited annually	3
NIST internal program assessment	The internal security program and practices are aligned with NIST	3
Vendor Management / Procurement	Vendor management and procurement practices include security reviews for each asset	5
Identify Maturity Level		3.2

CONFIDENTIAL – INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds 10

495/6 =82.5



399/5=79.8

InfoSec: DOIT

SECURITY INCIDENT IMPROVEMENT PLAN (SIIP)

Security Focus Area	Action	Owner	Target Timing	July 2019 Status
Process Improvements	Evaluate product, network and system security. • Checkmarx adoption / KPI • JIRA Security Tagging adoption / KPI • Vulnerability Scanning & Reviews with DOIT	T. Brown E. Quitugua K. Pierce	Ongoing	KPI creation: Underway DOIT vulnerability review: Ongoing
	Build Library of authoritative source of practices/processes, agreed to by engineering leadership	K. Pierce	• Q2-2019: List compiled • Q3-2019: Alignment with Engineering	Complete
	Improve Security Practice for the Company (SIIP)	T. Brown E. Quitugua K. Pierce	Ongoing	In Progress
Tools & Technology	Compile cumulative list of security tools and services for the organization (Security Tool Rationalization)	T. Brown E. Quitugua K. Pierce	Q2-2019	Complete
Training	Implement quarterly Incident Response Training	E. Quitugua	Ongoing Q2-Complete Q3- 8/19/19 Q4-TBD	In Progress
	Continue GDPR Bootcamp training. Refresh training materials	K. Pierce	Ongoing	Ongoing

CONFIDENTIAL – FOR INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved.

54